IN THE CLAIMS

Please amend the claims as follows:

1.   (currently amended) A method comprising ~~the steps of:~~

monitoring access points through which data can be exchanged with a network;

identifying an unauthorized access point~~; and~~

in response to an unauthorized access point being identified, determining make, model and default configuration password of said identified unauthorized access point by monitoring traffic passing through ~~the~~ said identified unauthorized access point;

addressing said identified unauthorized access point using said determined default configuration password; and

after gaining access thereto, reconfiguring said unauthorized access point to add an identity of said identified unauthorized access point to registers of ports for which charges are allocated such that access charges can be accumulated against said identity.

2.   (currently amended) ~~A~~ The method according to Claim 1, further comprising ~~the step of~~ determining ~~the~~ a geographical location of ~~the~~ said identified unauthorized access point.

3.   (currently amended) ~~A~~ The method according to one of Claims 1 and 2, further comprising ~~the step of~~ applying traffic filtering to monitored traffic passing through ~~the~~ said identified unauthorized access point.

4.   canceled

5.   (currently amended) ~~A~~ The method according to one of Claims 1 through 4 3, further comprising ~~the step of~~ accumulating charges for access and usage of network resources identified to ~~the~~ said identified unauthorized access point.

6.   (currently amended) ~~A~~ The method according to one of Claims 1 through 5, wherein ~~the step of~~ said identifying ~~an unauthorized access point comprises~~ further includes comparing ~~the identity~~ identities of monitored access points with a database of authorized access points.

7.   (currently amended) ~~A~~ The method according to Claim 6, wherein ~~the step of~~ said monitoring ~~comprises~~ further includes equipping each of a plurality of computer devices to detect access points accessible to ~~the~~ said computer devices and to report to a server computer system ~~the identity~~ identities of detected access points.

8.   (currently amended) ~~A~~ The method according to Claim 6, wherein ~~the step of~~ said monitoring ~~comprises~~ further includes querying network nodes for recent entries into node identifying connectivity tables maintained at ~~the~~ said network nodes.

9.   (currently amended) ~~A~~ The method according to one of Claims 7 and 8, wherein ~~the step of~~ said monitoring is performed intermittently and periodically.

10.   (currently amended) ~~A~~ The method according to Claim 9, wherein ~~the step of~~ said monitoring is performed at predetermined regular intervals.

11.   (currently amended) ~~A~~ The method according to Claim 9, wherein ~~the step of~~ said monitoring is performed at random irregular intervals.

12.   (currently amended) ~~A~~ The method according to Claim 2, wherein ~~the step of~~ said determining ~~the~~ geographic location ~~of an identified unauthorized access point comprises~~ further includes comparing ~~the~~ locations of a plurality of computer devices all of which report detection of ~~the~~ said identified unauthorized access point.

13.   (currently amended) ~~A~~ The method according to Claim 3, wherein ~~the step of~~ said applying ~~traffic filtering comprises~~ further includes denying access to ~~the~~ said network through ~~the~~ said identified unauthorized access point.

14.   (currently amended) A~~n~~ apparatus comprising:

a computer system;

a network interface connected to said computer system ~~and providing~~ to provide a communication channel between said computer system and a network; ~~and~~

~~program instructions stored accessibly to said computer system and cooperating with said computer system when executing on said computer system to~~ means for monitoring access points through which data can be exchanged with said network, ~~assist in identifying an unauthorized access point, and monitor traffic passing through an identified unauthorized access point;~~

means for identifying an unauthorized access point;

means for, in response to an unauthorized access point being identified, determining make, model and default configuration password of said identified unauthorized access point by monitoring traffic passing through said identified unauthorized access point;

means for addressing said identified unauthorized access point using said determined default configuration password; and

means for, after gaining access thereto, reconfiguring said unauthorized access point to add an identity of said identified unauthorized access point to registers of ports

for which charges are allocated such that access charges can be accumulated against said identity.

15.   (currently amended) The ~~A~~apparatus according to Claim 14, wherein said computer system is a workstation computer system ~~and further wherein said program instructions include an access point identification program cooperating therewith when executing on said system to identify access points accessible through said interface; and a reporting program cooperating with said identification program and with said system when executing on said system to report through said interface to a remote server computer system the identity of accessed points~~.

16.   (currently amended) The ~~A~~apparatus according to Claim 14, wherein said computer system is a server computer system ~~and further wherein said program instruction include a node identification database cooperating therewith when said program is executing on said system to identify unauthorized access points accessible to said system through said interface~~.

17.   (currently amended) The ~~A~~apparatus according to one of Claims 15 and 16, ~~and~~ further comprising a geographical location determining program effective when executing to derive ~~the~~ said physical location of an unauthorized access point.

18.   (currently amended) The ~~A~~apparatus according to one of Claims 15 through 17, ~~and~~ further comprising a traffic filter controlling program effective when executing to selectively impose a filter on traffic exchanged with ~~the~~ said network through an unauthorized node.

19.   canceled

20.   (currently amended) The ~~A~~apparatus according to one of Claims 15 through ~~19~~ 18, ~~and~~ further comprising an accounting control program effective when executing to accumulate charges for access and usage of network resources identified to ~~the~~ said identified unauthorized access point.

21.   (currently amended) A <u>computer storage medium having a computer</u> program product comprising:

~~a computer readable medium; and~~

~~program instructions stored on said medium accessibly to a computer system and~~ ~~effective when executing on a system to:~~

<u>computer program code for</u> monitor<u>ing</u> access points through which data can be exchanged with a network;

<u>computer program code for</u> identify<u>ing</u> an unauthorized access point<u>;</u>~~, and~~

<u>computer program code for, in response to an unauthorized access point being</u> <u>identified, determining make, model and default configuration password of said identified</u> <u>unauthorized access point by</u> monitor<u>ing</u> traffic passing through ~~the~~ <u>said</u> identified unauthorized access point<u>;</u>

<u>computer program code for addressing said identified unauthorized access point</u> <u>using said determined default configuration password; and</u>

<u>computer program code for, after gaining access thereto, reconfiguring said</u> <u>unauthorized access point to add an identity of said identified unauthorized access point</u> <u>to registers of ports for which charges are allocated such that access charges can be</u> <u>accumulated against said identity.</u>

22.   (currently amended) <u>The computer storage medium</u> ~~A program product~~ according to Claim 21<u>,</u> wherein <u>said computer storage medium</u> ~~the program instructions~~ further ~~comprise instructions~~ ~~effective to determine the~~ <u>includes computer program code for determining a</u> geographical location of ~~the~~ <u>said</u> identified unauthorized access point.

23.   (currently amended) <u>The computer storage medium</u> ~~A program product~~ according to one of Claims 21 and 22<u>,</u> wherein ~~the program instructions~~ <u>said computer storage medium</u> further ~~comprise instructions effective to~~ <u>includes computer program code for</u> apply<u>ing</u> traffic filtering to monitored traffic passing through ~~the~~ <u>said</u> identified unauthorized access point.

24.   canceled

25.   (currently amended) <u>The computer storage medium</u> ~~A program product~~ according to one of Claims 21 through ~~24~~ <u>23,</u> wherein ~~the program instructions~~ <u>said computer storage medium</u> further ~~comprise instructions effective to accumulate~~ <u>includes computer program code for accumulating</u> charges for access and usage of network resources identified to ~~the~~ <u>said</u> identified unauthorized access point.

26.   (currently amended) <u>The computer storage medium</u> ~~A program product~~ according to one of Claims 21 through 25<u>,</u> wherein ~~the program instructions~~ <u>said computer storage medium</u> further ~~comprise instructions effective to compare the~~ <u>includes computer program code for comparing</u> identity of monitored access points with a database of authorized access points.